AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1.-19. (Canceled)

20. (New) A digital information security system comprising:

a user application tool installed in a user terminal, the user application tool being structured to create a unique user key using unique system information of the user terminal, to transmit the unique user key to a server system via a network for registration and to subsequently transmit the unique user key to the server system via the network for authentication;

the server system comprising an encryption unit to encrypt digital information, a user information database to store the user information including the unique user key received from the user terminal for registration, a digital information database to store the encrypted digital information, a rule establishing unit to establish a rule corresponding to the user information and the digital information, a coupling unit to encrypt, using the unique user key, rule information corresponding to the rule, to encrypt, using the unique user key, a decryption key for decrypting the digital information, and to combine the encrypted rule information, the encrypted decryption key and the encrypted digital information into combined information, and a digital file database to store the combined information; and

the server system also comprising a server control unit including a user management tool to perform a user authentication process by comparing the unique user key stored in the user information database with the unique user key subsequently transmitted from the user terminal for authentication,

wherein the server control unit transmits the combined information from the digital file database to the user application tool after completing the user authentication process, when the user terminal requests a download of the digital information.

21. (New) The digital information security system as claimed in claim 20, wherein when the combined information is downloaded to the user application tool, it is determined

whether the digital file should be decrypted by determining whether the key used for encrypting the decryption key matches the unique user key created by the user application tool.

22. (New) The digital information security system as claimed in claim 20, wherein the rule establishing unit establishes a rule for one or more of authority of storage, authority of print, authority of allowable time for use, and authority of transfer of the digital file.

23. (New) The digital information security system as claimed in claim 20, wherein the system information includes wherein the unique system information includes at least one of unique CPU (Central Processing Unit) information, unique HDD (Hard Disk Drive) information, and serial number information of the user terminal.

24. (New) A digital information security method comprising the steps of:

creating a unique user key using unique system information of a user terminal using a user application tool installed in a user terminal;

transmitting digital information and user information including the unique user key from the user terminal to a server system via a network;

encrypting the digital information and the user information including the unique user key transmitted from the user terminal;

storing the encrypted user information and the encrypted digital information in the server system;

establishing a rule corresponding to the user information and the digital information;

encrypting the rule and a decryption key for decrypting the digital information using the unique user key;

combining the encrypted digital information, the encrypted rule and the encrypted decryption key into combined information;

storing the combined information;

performing a user authentication process by comparing the unique user key stored in the server with the unique user key subsequently transmitted from the user application tool of the user terminal for authentication;

transmitting the combined information from the server system to the user application tool via the network after completing the user authentication process, when the user terminal requests a download of the digital information; and

determining, with the user application tool, whether the digital file should be decrypted by determining whether the key used for encrypting the decryption key matches the unique user key created by the user application tool.

25. (New) The digital information security method as claimed in claim 24, wherein the rule includes one or more of authority of storage, authority of print, authority of allowable time for use, and authority of transfer of the digital information.

26. (New) The digital information security method as claimed in claim 24, wherein the unique system information includes at least one of unique CPU (Central Processing Unit) information, unique HDD (Hard Disk Drive) information, and serial number information of the user terminal.

27. (New) A digital information encryption and upload method comprising the steps of:

creating a unique user key using unique system information of a user terminal using a user application tool installed in a user terminal;

uploading digital information, user information including the unique user key from the user terminal to a server system;

encrypting the digital information and the user information including the unique user key transmitted from the user terminal;

storing the encrypted user information and the encrypted digital information in the server system;

establishing a rule corresponding to the user information and the digital information;

encrypting the rule and a decryption key for decrypting the digital information using the unique user key;

combining the encrypted decryption key, the encrypted digital information, and the encrypted rule into a combined file; and

storing the combined file.

28. (New) The digital information encryption and upload method as claimed in claim 27, wherein the rule includes one or more of authority of storage, authority of print, authority of allowable time for use, and authority of transfer of the digital information.

29. (New) The digital information encryption and upload method as claimed in claim 27, wherein the unique system information includes at least one of unique CPU (Central Processing Unit) information, unique HDD (Hard Disk Drive) information, and serial number information of the user terminal.

30. (New) An encrypted digital information download method comprising the steps of:

creating a unique user key using unique system information of a user terminal using a user application tool installed in a user terminal;

transmitting a request from the user terminal to a server system to download digital information from the server system;

transmitting the unique user key from the user terminal to the server system;

performing a user authentication process at the server system by comparing a unique user key stored in the server system with the unique user key transmitted from the user terminal;

transmitting a digital file from the server to the user terminal when the user terminal is authenticated, the digital file including an encrypted version of the digital information and an

encrypted decryption key, the decryption key for decrypting the encrypted version of the digital information; and

decrypting, at the user terminal, the encrypted version of the digital information if the key used for encrypting the decryption key matches the unique user key created by the user application tool,

31. (New) The digital information download method as claimed in claim 30, further comprising:

establishing a rule associated with the digital information, wherein the rule includes one or more of authority of storage, authority of print, authority of allowable time for use, and authority of transfer of the digital information;

wherein the digital file includes an encrypted version of the rule.

32. (New) The digital information download method as claimed in claim 30, wherein the unique system information includes at least one of unique CPU (Central Processing Unit) information, unique HDD (Hard Disk Drive) information, and serial number information of the user terminal.

33. (New) A digital information security method in a system in which a digital information server and a plurality of user systems are connected via a network,

receiving, at the digital information server, a download request from one user system of the plurality of user systems, the download request for digital information;

combining into a file an encrypted version of the digital information, a decryption key for decrypting the encrypted version of the digital information, and a rule corresponding to the digital information, wherein the rule corresponding to the digital information includes authority of use of the digital information and includes authority of transfer indicating whether the one user system can transfer the digital information to another user system;

transmitting the file from the digital information server to the one user system in response to the download request;

decrypting at the one user system the encrypted version of the digital information by the use of the decryption key; and

utilizing at the one user system the digital information in accordance with the rule corresponding to the digital information, and

transferring the digital information from the one user system to another user system in accordance with the rule corresponding to the digital information.

34. (New) The digital information security method as claimed in claim 33, further comprising:

setting, using the digital information server, a plurality of groups, each group including a plurality of user systems; and

establishing, using the digital information server, a plurality of rules, each rule of the plurality of rules corresponding to each group;

wherein the one user system is in one of the groups, wherein the rule corresponding to the digital information includes the rule corresponding to the group;.

35. (New) The digital information security method as claimed in claim 33, wherein the decryption key in the file and the rule corresponding to the group in the file are encrypted.

36. (New) The digital information security method as claimed in claim 35, wherein the decryption key in the file and the rule corresponding to the group in the file may be decrypted using a unique user key created using unique system information of the one user system.

37. (New) the digital information security method as claimed in claim 36, wherein the unique system information includes at least one of unique CPU (Central Processing Unit) information, unique HDD (Hard Disk Drive) information, and serial number information of the one user system.